2400
2631 03-CO

#4
10-8-02
JM

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Post Office as first class mail in an envelope addressed to: Commissioner for Patents, Washington, D.C. 20231, on

Date: 1-24-02
Name: Melissa Scanzillo
Signature: Melissa Scanzillo
Clifford Chance Rogers & Wells LLP

COPY OF PAPERS ORIGINALLY FILED

Docket No. 6208-027

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Imazu		
Filed:	November 29, 2001	Group Art Unit:	to be determined
Serial No:	09/997,092	Examiner:	to be determined
For:	AUTHENTICATION METHOD AND DEVICE		

Commissioner for Patents
Washington, D.C. 20231

SUBMISSION OF PRIORITY DOCUMENT UNDER 35 USC §119

Sir:

Enclosed please find the certified true copy of Japanese patent application no. 2000-402152 filed December 28, 2000. Applicant respectfully requests that the priority claim made to this Japanese patent application under 35 USC §119 be accepted and the attached document be placed in the file for the above matter.

The Commissioner is hereby authorized to charge any fees required with this submission to Deposit Account No. 50-0521.

Respectfully submitted,

Date: 1/23/02

Joseph Levi
Reg. No. 41,152

Clifford Chance Rogers & Wells LLP
200 Park Avenue
New York, NY 10166-0153
Telephone: (212) 878-8564

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月２８日

出願番号
Application Number: 特願２０００－４０２１５２

出願人
Applicant(s): モルガン・スタンレー・ディーン・ウィッター・ジャパン・リミテッド

２００１年１１月３０日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願

【整理番号】　10444001

【提出日】　平成12年12月28日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L　9/00675

【発明者】

【住所又は居所】　東京都渋谷区恵比寿４－２０－３ＹＧＰタワー　モルガン・スタンレー・ディーン・ウィッター・ジャパン・リミテッド内

【氏名】　今津　英世

【特許出願人】

【住所又は居所】　東京都渋谷区恵比寿４－２０－３ＹＧＰタワー

【氏名又は名称】　モルガン・スタンレー・ディーン・ウィッター・ジャパン・リミテッド

【代理人】

【識別番号】　100110412

【弁理士】

【氏名又は名称】　藤元　亮輔

【電話番号】　03-3523-1227

【手数料の表示】

【予納台帳番号】　062488

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証方法及び装置

【特許請求の範囲】

【請求項１】　ユーザの通信装置に登録用画面のアドレスを送信するステップであって、前期アドレスは前記ユーザ及び／又は前記通信装置を識別する登録用識別子を含んだステップと、

前記アドレスがアクセスされて前記登録用画面に第１のパスワードが入力されて返信された場合に前記登録用識別子と前記第１のパスワードに基づいて前記ユーザを認証するステップと、

前記認証ステップが成功した場合に、ログイン画面を前記ユーザに送信するステップであって、前記ログイン画面は、第２のパスワードが入力されるフィールドと、前記ユーザ及び／又は前記通信装置を識別するログイン用識別子とを有するステップと、

前記ユーザにより返信された前記ログイン画面に含まれる前記ログイン用識別子と前記第２のパスワードに基づいて前記ユーザを認証するステップとを有する認証方法。

【請求項２】　前記登録用識別子と前記ログイン用識別子は異なる請求項１記載の認証方法。

【請求項３】　前記第１及び第２のパスワードは同一である請求項１記載の認証方法。

【請求項４】　前記ログイン画面の前記ログイン用識別子は、前記通信装置が自動的に発信する当該通信装置を独自に識別する装置識別子である請求項１記載の認証方法。

【請求項５】　前記ログイン画面を前記ユーザに送信するステップは、前記ログイン画面の内容を前記通信装置に保存することを可能にする請求項１記載の認証方法。

【請求項６】　前記ログイン画面のアドレスが前記ログイン用識別子を含み

前記ログイン画面を前記ユーザに送信するステップは、当該アドレスを前記通

信装置に保存することを可能にする請求項１記載の認証方法。

【請求項７】　前記登録画面への返信による認証ステップは当該認証が成功した場合に前記登録画面へのアクセスができなくなる請求項１記載の認証方法。

【請求項８】　前記登録用画面に前記第１のパスワードが入力されて返信された際に、当該返信が所定の時間内に行われた場合のみ受け付ける請求項１記載の認証方法。

【請求項９】　ユーザと、登録用識別子と、登録用パスワード検証用情報と、ログイン用識別子と、ログイン用パスワード検証用情報とを関連付けて格納する記憶部と、

ユーザの通信装置に登録用画面のアドレスを送信する制御部であって、前期アドレスは前記ユーザ及び／又は前記通信装置を識別する登録用識別子を含んだ第１の制御部と、

前記通信装置からの登録用画面要求に対して、登録用パスワードが入力されるフィールドと、前記登録用識別子とを有する登録用画面を前記通信装置に提供すると共に、前記登録用画面に前記ユーザが前記登録用パスワードを入力して返信した場合に前記記憶部を参照して前記ユーザを認証する第２の制御部と、

前記認証が成功した場合に、ログイン用パスワードが入力されるフィールドと、前記ログイン用識別子とを有するログイン画面を前記通信装置に提供すると共に、前記ログイン画面に前記ユーザが前記ログイン用パスワードを入力して返信した場合に前記記憶部を参照して前記ユーザを認証する第３の制御部とを有する認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、一般には、デジタル情報の伝送に係り、特に、システムの利用者の身元又は権限の照合のための手段を含む秘密又は安全な通信のための配置に関する。本発明は、例えば、携帯電話、自動車電話、ＰＨＳ（Ｐｅｒｓｏｎａｌ Ｈａｎｄｙ－ｐｈｏｎｅ Ｓｙｓｔｅｍ）、ＰＤＡ（パーソナル・デジタル・アシスタンツ）などの小型携帯端末のユーザ（クライアント）が、インターネットな

どのネットワークを利用して、所望の情報を格納するサーバにアクセスする際の認証方法及び装置に好適である。

【０００２】

【従来の技術】

ＩＴ技術革新により、インターネットをベースとしたグローバルな世界が展開され、その利便性が大きくクローズアップされてきている。情報のデジタル化とインターネットが結びついた情報社会は、企業活動から個人の生活に至るまで大きく変えてきている。ユーザはインターネットに接続されている様々なサーバに同時にアクセスして多種多様なデータやサービスを得ることができる。また、最近ではインターネットにアクセス可能な端末はデスクトップパーソナルコンピュータ（ＰＣ）だけでなく、携帯電話やＰＤＡなどの小型携帯端末をも含むようになってきた。

【０００３】

インターネットによって個人や企業が接続されると、情報（例えば、商業目的から特定の会員にのみ提供される音楽情報や、企業が外部に漏らしたくないその顧客情報）の提供や電子商取引（例えば、クレジットカード情報の送信を要するオンラインショッピング）を安全に行う需要が高まる。情報にアクセスするユーザを制限したいサイトは、通常、ユーザをオンライン又はオフラインで登録し、登録されたユーザにのみ情報へのアクセスを許容するシステムを採用する。

【０００４】

安全な通信には暗号が使用される。暗号には守秘と認証がある。守秘は、平文を暗号文に変換する暗号化と暗号文を平文に変換する復号化からなり、暗号化及び復号化を決定するのはアルゴリズム（暗号方式）と鍵である。小型情報機器は、通常、電子メールを暗号化及び復号化できないがＷＷＷ（以下、単に「ウェブ」という。）通信は暗号化及び復号化することができる守秘通信環境を有する。認証は、本物かどうかを確認する対象により、本人確認、メッセージ認証、デジタル署名に大別することができる。本人確認は、相手認証又はユーザ認証とも呼ばれ、マルチユーザーのコンピュータシステムやネットワークシステムにおいて通信相手が本物であることを確認する技術であり、単純な方法としてパスワード

を利用する。典型的に、本人確認は、ユーザが設定して予めサーバ（の記憶部のアクセス権限リスト）に登録されたユーザＩＤ（又はユーザ名）とパスワードの組み合わせを利用し、ユーザはコンピュータシステムやネットワークにログインする際に、ユーザＩＤとパスワードの入力が要求される。ユーザが両方のデータを入力すると、それが予めサーバ（の記憶部のアクセス権限リスト）に登録されたものかどうかの認証が両者を照合することによってなされ、認証された場合にのみアクセス権限リストに登録された範囲でシステムの使用が許可される。ここで、ユーザＩＤはシステムにおけるユーザの識別名であり、パスワードはユーザが任意に設定した数字やアルファベットなどの文字列である。

【０００５】

【発明が解決しようとする課題】

しかし、小型携帯端末を利用するユーザはキー入力を通常指一本で行うために、ユーザＩＤ及びパスワード、インターネットのＵＲＬなど多くのキー入力操作を要求する従来の認証方法は、これらを入力及び管理する上でユーザにとって負担となる。その一方、安全な通信を実現するためにユーザＩＤ及びパスワードを利用する認証方法が達成できるセキュリティを維持する必要がある。また、ＰＣと異なり小型携帯端末は利用可能な暗号が制限されている場合が多い。例えば、携帯電話は、電子メール通信に暗号を使用できないがＷＷＷ（以下、単に「ウェブ」という。）通信には暗号を使用できる。ユーザ識別部を含んだログインのためのＵＲＬを電子メールで小型携帯端末に送信することでユーザの便宜を図ることができるが、電子メールが暗号化できない場合、そのユーザ用のＵＲＬを盗み見られる恐れが生ずる。

【０００６】

これに対して、ユーザＩＤとパスワードに加えて又はこれらに代えてユーザの身体的特徴（例えば、指紋、掌紋、声紋、網膜パターンといった身体的な特徴や、筆跡やキータイプの際の癖）を利用するバイオメトリックス（生体認証）も提案されている。バイオメトリックスを使用すればセキュリティは向上するが、生体情報を読み取る専用のハードウェア（例えば、指紋読取装置）の購入はユーザにとって負担になる。また、認証装置側がサポートしている生体情報のみしか利

用することができない。

【０００７】

そこで、本発明は、このような従来の課題を解決する新規かつ有用な認証方法及び装置を提供することを概括的な目的とする。

【０００８】

より特定的には、本発明は、ユーザを容易に、比較的安価に、安全に認証することができる認証方法及び装置を提供することを例示的目的とする。

【０００９】

また、本発明は、小型情報機器を使用するユーザのキー操作をなるべく減少してユーザの負担を軽減する認証方法及び装置を提供することを他の例示的目的とする。

【００１０】

【課題を解決するための手段】

上記目的を達成するために、本発明の一側面としての認証方法は、ユーザの通信装置に登録用画面のアドレスを送信するステップであって、前記アドレスは前記ユーザ及び／又は前記通信装置を識別する登録用識別子を含んだステップと、前記アドレスがアクセスされて前記登録用画面に第１のパスワードが入力されて返信された場合に前記登録用識別子と前記第１のパスワードに基づいて前記ユーザを認証するステップと、前記認証ステップが成功した場合に、ログイン画面を前記ユーザに送信するステップであって、前記ログイン画面は、第２のパスワードが入力されるフィールドと、前記ユーザ及び／又は前記通信装置を識別するログイン用識別子とを有するステップと、前記ユーザにより返信された前記ログイン画面に含まれる前記ログイン用識別子と前記第２のパスワードに基づいて前記ユーザを認証するステップとを有する。かかる認証方法によれば、登録用画面と第１のパスワードを利用したステップを経ることによってユーザはログイン画面に識別子をキー入力及び識別子を管理する負担から開放され、小型携帯端末のユーザにとっては特に便宜である。なおかつ、本認証方法は、識別子と（第２の）パスワードを利用する認証と同程度のセキュリティを維持することができる。登録用画面のアドレスが暗号を使わずに送信された結果として漏洩しても、第１の

パスワードが正規のユーザであることを担保している。

【００１１】

前記登録用識別子と前記ログイン用識別子は異なることが好ましい。ログイン用識別子を登録用識別子から推定不可能にすることにより登録用画面のアドレスがログインの手がかりとなることを防ぐことができる。前記第１及び第２のパスワードは同一であってもよいし、異なってもよい。同一の場合はユーザによるパスワード管理の負担を軽減することができる。

【００１２】

前記ログイン画面の前記識別子は、前記通信装置が自動的に発信する当該通信装置を独自に識別する装置識別子であってもよい。特定の携帯電話などはユーザの操作とは無関係に通信サービスの一環として装置識別子（即ち、携帯電話の独自の識別子）をサーバに通知するものがある。装置識別子は、同一の機種であっても別個に割り当てられるため、結局は機種とその機種を使用するユーザの両方を特定している。このため、かかる識別子を利用すればログイン画面から通信装置の識別子を独立して設定することを省略することができる。

【００１３】

前記ログイン画面を前記ユーザに送信するステップは、前記ログイン画面の内容を前記通信装置に保存することを可能にすることができる。これは、通信装置がログイン画面を保存することが可能な場合に行われる。代替的に、前記ログイン画面のアドレスが前記識別子を含み、前記ログイン画面を前記ユーザに送信するステップは、当該アドレスを前記通信装置に保存することを可能にしてもよい。この場合、例えば、通信装置は、識別子を含んだログイン画面のＵＲＬをブックマークすることができる。

【００１４】

前記登録画面に前記第１のパスワードが入力されて返信され、認証が成功した際に、当該登録画面へのアクセスを禁止してもよい。これにより、登録画面のアドレスを盗み見た者が登録を試みても正規ユーザが登録を済ませていれば登録は不可能になり、セキュリティが向上する。一方盗み見た者が先に登録を済ませてしまった場合でも、正規ユーザは登録画面にアクセスできないことにより異常を

知ることができ、登録のやり直し等の対策をいち早くとることができる。前記登録用画面に前記第１のパスワードが入力されて返信された際に、当該返信が所定の時間内に行われた場合のみ受け付けてもよい。これにより、第１のパスワードを利用したユーザの認証は、登録用画面にパスワードが所定時間内に入力されて返信された場合に行われる。正規のユーザ以外の者が登録用画面を取得しても第1のパスワードを探っている間に期限が切れてしまうためにセキュリティが向上する。

【００１５】

本発明の別の側面としての認証装置は、ユーザと、登録用識別子と、登録用パスワード検証用情報と、ログイン用識別子と、ログイン用パスワード検証用情報とを関連付けて格納する記憶部と、ユーザの通信装置に登録用画面のアドレスを送信する制御部であって、前期アドレスは前記ユーザ及び／又は前記通信装置を識別する登録用識別子を含んだ第１の制御部と、前記通信装置からの登録用画面要求に対して、登録用パスワードが入力されるフィールドと、前記登録用識別子とを有する登録用画面を前記ユーザに提供すると共に、前記登録用画面に前記ユーザが前記登録用パスワードを入力して返信した場合に前記記憶部を参照して前記ユーザを認証する第２の制御部と、前記認証が成功した場合に、ログイン用パスワードが入力されるフィールドと、前記ログイン用識別子とを有するログイン画面を前記ユーザに提供すると共に、前記ログイン画面に前記ユーザが前記ログイン用パスワードを入力して返信した場合に前記記憶部を参照して前記ユーザを認証する第３の制御部とを有する。かかる認証装置は第２の制御部を介して登録制御を行い、第３の制御部を介してログイン制御を行う。第１・第２・第３の制御部は同一であってもよいし、いずれか２つの制御部が同一であってもよい。登録制御を経て提供されるログイン画面にはログイン用識別子を有するのでユーザはこれらをキー入力及び管理する負担から開放され、小型携帯端末のユーザにとっては特に便宜である。登録用画面の送受信は、仮に、暗号を使用しなくても登録用パスワードが通信相手が正規のユーザであることを担保している。登録用パスワードとログイン用パスワードは同一であってもよいし、異なってもよい。なお、前記登録用識別子と前記ログイン用識別子は異なることが好ましい。ログイ

ン用識別子を登録用識別子から推定不可能にすることにより登録用画面のアドレスがログインの手がかりとなることを防ぐことができる。

【００１６】

本発明の他の目的と更なる特徴は、以下、添付図面を参照して説明される実施例において明らかになるであろう。

【００１７】

【発明の実施の形態】

以下、添付図面を参照して、本発明の認証システム１について説明する。ここで、図１は、本発明の認証システム１の概念的なシステム構成図である。図１に示すように、認証システム１は、インターネット３０に接続された複数のユーザ（クライアント）１０（なお、参照番号「１０」は１０Ａ、１０Ｂなどを総括するものとする。）と、情報提供装置２０と、認証装置１００とを有する。

【００１８】

ユーザ１０は、個人、法人を問わず、また設置場所の国内外を問わないが、典型的には、個人又は企業ユーザが操作するプラットフォーム又はそれに格納されたソフトウェアを指し、本実施例ではユーザ本人を表す場合もある。プラットフォームは情報を送受信、加工及び格納する機器としてＰＣのみならず、デジタルテレビ、ＰＤＡ、自動車電話、携帯電話、ＰＨＳ、ＷＡＰ（Ｗｉｒｅｌｅｓｓ Ａｐｐｌｉｃａｔｉｏｎ）、ゲーム機などを広く含む。但し、本実施例のユーザ１０は、画面メモ機能を有する携帯電話及びにそれに格納されたソフトウェアを使用する。画面メモ機能は、画像を取り込んで保存する機能であり、ドコモ社製ｉモード携帯電話などにおいて広く使用されている。

【００１９】

ユーザ１０はインターネット３０を介して情報提供装置２０及び認証装置１００と交信するためのブラウザを格納している。ブラウザはクライアント１０にＥメールの使用を可能にしている。従って、クライアント１０は、無線通信により情報提供装置２０及び認証装置１００と交信してもよいし、インターネットを利用してこれらと交信してもよい。かかるブラウザは、情報提供装置２０及び認証装置１００のＵＲＬをブックマークできるので好ましい。

【００２０】

情報提供装置２０は、ユーザ１０が希望する情報及び／又はサービスを格納している。情報提供装置２０は、一般に、商業的理由及び／又は情報の機密性から特定のユーザにのみアクセスを許容するためにユーザがログインする際にユーザの認証を必要とする。例えば、会員のみが株予想、出会い、競馬予想などの所定の情報にアクセスが許容される場合やオペレータのみが企業の機密情報にアクセスが許容される場合などである。情報提供装置２０は、後述する認証装置１００の機能を有して一体的に構成又はインターネット３０を介さずにこれに接続されてもよい。情報提供装置２０は、後述する認証装置１００のハードウェア構成要素を一般に有しているので、ここでは詳しい説明は省略する。

【００２１】

インターネット３０はネットワークの典型例であるが、本発明は、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＭＡＮ（Ｍｅｔｒｏｐｏｌｉｔａｎ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）、商業専用回線（アメリカオンライン等）その他のオンラインネットワークに使用されることを妨げるものではない。

【００２２】

認証装置１００は、ＣＰＵ１１０と、通信ポート１２０と、乱数発生器１３０、メモリ１４０と、暗号／復号化部１５０、記憶部（データ記憶装置）２００とを有する。なお、認証装置１００は、メールサーバーやニュースサーバーとして機能することもできる。ＣＰＵ１１０は、ＭＰＵなど名称の如何を問わない処理装置を広く含み、認証装置１００の各部を制御する。認証装置１００は、ＣＰＵ１１０により制御され、データ記憶装置２００の各種データベースを処理する専用の処理装置を含んでもよい。また、認証装置１００は、図示しない入力手段（キーボード、マウスその他のポインティングデバイス）、ディスプレイなどを有する。入力手段を介して認証装置１００のオペレータは記憶部２００に各種データを入力したり、必要なソフトウェアをメモリ１５０や記憶部２００にセットアップしたりすることができる。

【００２３】

必要があれば、認証装置１００は、ＬＡＮその他のネットワークを介して他のコンピュータに接続され、ＣＰＵ１１０はそれらのコンピュータと通信することができる。ＣＰＵ１１０は、本発明との関係では、記憶部２００に格納されているデータベース各種（ユーザ管理テーブル２１０、登録用画面管理テーブル２２０及びログイン画面管理テーブル２３０）の構築と、当該データベースを利用してユーザ１０の認証をすることができる。

【００２４】

通信ポート１２０は、インターネットに（必要があれば、インターネット・サビス・プロバイダ（ＩＳＰ）を介して）接続される公衆電話回線網、ＩＳＤＮ、各種専用線にモデム、ターミナルアダプタ（ＴＡ）などを介して接続可能なＵＳＢポートやＩＥＥＥ１３９４ポートなどを含む。また、通信ポート１２０は、認証装置１００がＬＡＮに接続される場合には、ハブやルーターなども含むものである。

【００２５】

乱数発生部１３０は、乱数を発生させる関数を持つプログラム言語を有する。本発明では、ＩＤはユーザ１０が決定するのではなく、乱数発生部１３０で発生させた乱数を元に、ＣＰＵ１１０がユーザ１０にランダムなＩＤを割り当てる。

【００２６】

暗号／復号化部１４０は、ユーザ１０の設定したパスワードを記憶部２００に格納したり、ネットワーク上でデータを送受信したりする際に、第三者が理解できないように変換（暗号化）し、また、認証装置１００がユーザ１０の認証を行う際、記憶部２００から取り出した暗号化されたユーザ１０のパスワードを解読可能に変換する（復号化）。これらの暗号化と複合化を決定するものは、手順（アルゴリズム）と、不規則に並んだ英数字や記号のパラメータ（文字列）となる鍵である。ハードウェアやソフトウェアの固定部分が手順で、変更可能な文字列が鍵となる。手順の仕組み（暗号方式）は、同一の鍵を送信者と受信者が秘密に共有する秘密鍵暗号でも、暗号化鍵と復号化鍵が異なり、暗号化鍵は公開し、復号化鍵は受信者が秘密に保持する公開鍵暗号でもよい。なお、本発明には当業界で周知のいかなる暗号技術をも適用することができるので、ここでは詳しい暗号

について説明は省略する。

【００２７】

メモリ１５０は、ＲＡＭやＲＯＭを含み、記憶部２００などから読み出すデータ又は記憶部２００などへ書き込むデータを一時的に記憶する。メモリ１５０は、ＣＰＵ１１０の動作に必要な各種ソフトウェアやファームウェアその他のソフトウェアを格納する。

【００２８】

メーラー１６０は、ユーザ１０と電子メールを送受信するソフトウェアであり、ユーザ１０その他の外部から受信したメールを格納する受信トレイ、ユーザ１０その他の外部に送信する予定のメールを格納する送信トレイ、既に外部に送信済みのメールを格納する送信済みトレイ、任意のトレイから削除したメールを格納する削除済みトレイ、草案段階のメールを格納する下書きトレイなどの図示しない記憶部を含む。本実施例では、認証装置１００のメールサーバーは認証装置１００とは別に設けられているが、上述したように、認証装置１００がメールサーバーとして機能してもよい。メーラー１６０は、定型文などのメッセージ（例えば、「ご利用ありがとうございます。下記の登録用画面（又はアクティベーション画面）に３時間以内にアクセスして下さい。」）と、ユーザの端末１０に固有の登録用画面のＵＲＬ（即ち、後述する登録用識別子を含んだＵＲＬ）、その他の情報をユーザ１０に送信する。ここで、「ユーザの端末に固有の登録用画面」としたのは、携帯電話は機種によって受信可能なサイトのフォーマットが異なるために、後述する登録用画面のうちユーザの携帯電話の機種に適合するものが使用される必要があるからである。もっとも、本発明は、認証装置１００がメーラー１６０を有することを本質的に要求するものではない。

【００２９】

記憶部２００はユーザ管理テーブル２１０、登録用画面管理テーブル２２０及びログイン画面管理テーブル２３０のデータベースを含んでいるが、これらに限定されるものではない。

【００３０】

ユーザ管理テーブル２１０は、例示的に、ユーザ１０の氏名、住所、性別、年

齢、誕生日、電話番号、電子メールアドレス、使用される携帯電話の機種、一又は複数のパスワードの検証用情報（パスワード自体であってもよいが、これを検証するのに必要なすべての情報を含む）、携帯電話の機種に対応した処理の種類、銀行口座番号、クレジットカード番号、暗号用の鍵、その他のＩＤ情報を格納している。ここで、「携帯電話の機種に対応した処理の種類」は、必ずしも常に必要ではないが、携帯電話の機種に応じて表示可能なウェブ上の画面のフォーマットが変わる場合や保存機能が変わる場合（例えば、あるウェブ上の画面の内容を保存することはできないが、そのＵＲＬのブックマークはできるなど）に当該携帯電話に適合する処理（例えば、ウェブ画面を当該携帯電話に適合するフォーマットにしてＵＲＬに所定の識別子を挿入するなど）を行う。ユーザ１０の登録は、予めユーザ１０のＩＤ情報を認証装置２００及びその管理者が当該携帯電話を利用したり、郵送、ＦＡＸを利用したりするなどオフラインで行い、その後、オンラインでユーザ１０の接続要求に対して認証装置２００が、ユーザ１０の登録を再度行う。オンラインでの登録作業は、ＣＰＵ１１０が用意した所定の登録フォームにクライアント１０が入力して送信する。ユーザ１０は、自己の端末を利用して、いつでも自分のＩＤ情報を確認して必要があれば変更することができる。

【００３１】

ＣＰＵ１１０は、ユーザ管理テーブル２１０を参照して、ユーザ１０が認証装置１００にアクセスを希望する際にユーザ１０を認証する。また、ユーザ１０が登録内容を更新又は削除する場合などは更に追加的な認証を行ってもよい。なお、必要があれば、認証装置１００は、ユーザ１０の声紋により認証する声紋認証装置を備えてもよく、この場合は上記ＩＤ情報はユーザ１０の声紋を含む。

【００３２】

登録用画面管理テーブル２２０は、ユーザ及び／又はユーザが使用する通信装置（本実施例では、携帯電話）固有の登録用画面である登録用画面２２１を格納している。登録用画面２２１は、後述するように、ＣＰＵ１１０によって、予め登録されているユーザ１０の携帯電話の電子メールアドレスに電子メールで提供される。かかる登録用画面２２１の提供は時間的に制限することが好ましい。こ

れにより、後述するように、正規のユーザ以外の者（不正者）が登録用画面２２１のＵＲＬを取得しても登録用パスワードを探っている間に期限が切れてしまうためにセキュリティが向上する。

【００３３】

登録用画面２２１（なお、参照番号「２２１」は２２１ａ、２２１ｂなどを総括するものとする。）は、図２（ａ）乃至（ｄ）に示すように、幾つかの種類とフィールドを有する。ここで、図２は、認証装置１００からウェブ通信によりユーザ１０に提供される登録用画面２２１の概略ブロック図である。同図において、図２（ａ）は、ユーザ１０に最初に提供される登録用画面２２１ａを示す。図２（ｂ）は、正規のユーザ１０が登録用画面２２１ａに誤った登録用パスワードを入力及び返信した場合に提供される登録用画面２２１ｃを示す。図２（ｃ）は、正規のユーザ１０が登録用画面２２１ａに登録用パスワードを有効期限が切れた後に入力及び返信した場合に提供される登録用画面２２１ｄを示す。図２（ｄ）は、ユーザ管理テーブル２１０に登録されたユーザ及び／又は通信装置と同一の機種を使用しない者が登録用画面２２１ａに登録用パスワードを入力及び返信した場合に提供される登録用画面２２１ｄを示す。

【００３４】

まず、図２（ａ）を参照するに、登録用画面２２１ａは、登録用識別子２２２と、登録用パスワード２２３と、送信ボタン２２４と、有効期限２２５のフィールドを有する。但し、登録用画面管理テーブル２２０には登録用識別子２２２と有効期限２２５が入力される予定の（即ち、入力される前の）登録用画面２２１ａが格納される。フィールド２２２は、ユーザ管理テーブル２１０に登録されたユーザ及び／又はその通信装置を識別する識別子である。登録用識別子２２２は、登録用画面２２１ａを受け取った者から隠された不可視の状態で、又は、登録用画面２２１ａを受け取った者が確認できるように、登録用画面２２１ａに埋め込まれている。本実施例では、上述したように、登録用識別子２２２はメーラー１６０によってユーザ１０に送られるものをそのまま使用しているが、別の識別子を使用してもよい。登録用識別子２２２が登録用画面２２１ａに既に埋め込まれているので、ユーザ１０はこれを入力及び管理する負担から開放される。フィ

ールド２２３は、ユーザが予め任意に決定してユーザ管理テーブル２１０に登録した（例えば、８桁の）登録用パスワードを入力するフィールドである。フィールド２２４は、ユーザが登録用パスワードを入力し終わった後にこれを認証装置１００にウェブ通信により返信するためにクリックされるフィールドである。フィールド２２５は、ユーザ１０が確認できる状態又は隠された不可視の状態で形成され、ユーザ１０がメーラー１６０からメッセージを受信してから登録用パスワードを入力しなければならない有効期限（例えば、３時間）を表すフィールドである。なお、有効期限２２５の始期と終期は任意の時間を選択することができる。

【００３５】

図２（ｂ）を参照するに、登録用画面２２１ｂは、メッセージ２２６と、「戻る」ボタン２２７のフィールドを有する。メッセージ２２６は、入力された登録用パスワードが間違っている旨及び再試行を促す旨をユーザ１０に表示する。「戻る」ボタン２２７は、登録用画面２２１ｂを２２１ａに切り替えてユーザ１０にパスワードの再入力を可能にするボタンである。

【００３６】

図２（ｃ）を参照するに、登録用画面２２１ｃは、メッセージ２２８のフィールドを有する。メッセージ２２８は、設定された有効期限が過ぎている旨をユーザ１０に通知する。本実施例では、登録用画面２２１ｃは、登録用画面２２１ａに入力された登録用パスワード２２３が正しいか誤っているかに拘らず有効期限が過ぎていれば登録用画面２２１ｂに優先して提供されるように構成されている。

【００３７】

図２（ｄ）を参照するに、登録用画面２２１ｄは、メッセージ２２９のフィールドを有する。メッセージ２２９は、使用された携帯電話の機種が予めユーザ保管データベース２１０に登録された機種とは異なる旨をユーザ１０に通知する。登録用画面２２１ｄはユーザの携帯電話１０が自動的に装置識別子（即ち、携帯電話の独自の識別子）を認証装置１００に通知する場合に提供される。例えば、ユーザ１０Ａに送信される登録用画面２２１ａのＵＲＬと登録用パスワードをユ

ーザ１０Ｂが入手して登録用画面２２１ａを取得して登録用パスワードを入力して返信した場合について考える。ユーザ１０Ｂの携帯電話が自動的に装置識別子を認証装置１００に通知する機種であれば、制御部１１０は、ユーザ１０Ｂの装置識別子が登録用識別子２２２又はユーザ管理テーブル２１０に格納されたその他の検証用情報に基づいてユーザ１０ｂの装置識別子がユーザ１０Ａのそれとは異なることを検証することができる。この結果、ユーザ１０Ｂに後述するログイン画面２３１ａを送信することを防止することができる。

【００３８】

ログイン画面管理テーブル２３０は、ユーザ及び／又は通信装置（本実施例では携帯電話）を識別するログイン用識別子がユーザ１０からは隠れた状態で埋め込まれる予定の（即ち、埋め込まれる前の）ログイン画面２３１（なお、参照番号「２３１」は２３１ａ、２３１ｂなどを総括するものとする。）を格納している。ユーザ１０に提供されるログイン画面２３１には識別子が埋め込まれているために、ユーザ１０はこれを携帯電話から入力する必要がないためキー操作の軽減に寄与する。また、携帯電話上のログイン画面２３１を不心得者が盗み見ても識別子を認識することはできないのでセキュリティは向上する。

【００３９】

ログイン画面２３１は、図３（ａ）及び（ｂ）に示すように、幾つかの種類とフィールドを有する。ここで、図３は、認証装置１００からウェブ通信によりユーザ１０に提供されるログイン画面２２１の概略ブロック図である。同図において、図３（ａ）は、正規のユーザ１０が登録用画面２２１ａに正しいパスワードを有効期限が切れる前に入力及び返信した結果、制御部１１０によって認証された場合に提供されるログイン画面２３１ａを示す。図３（ｂ）は、正規のユーザ１０が登録用画面２３１ａに誤ったログイン用パスワードを入力及び返信した場合に提供されるログイン画面２３１ｂを示す。

【００４０】

まず、図３（ａ）を参照するに、ログイン画面２３１ａは、ログイン用識別子２３２と、パスワード２３３と、送信ボタン２３７のフィールドを有する。但し、ログイン用画面保管テーブル２２０にはログイン用識別子２３２が入力される

予定の（即ち、入力される前の）ログイン画面２３１ａが格納される。ログイン用識別子２３２が入力されたログイン画面２３１ａの内容はユーザの携帯電話１０に保存されるか、又は、ログイン識別子２３２を一部又は全部若しくはこれに関連する情報を含んだログイン画面２３１ａのＵＲＬはユーザの携帯電話１０によって保存（ブックマーク）される。

【００４１】

フィールド２３２はユーザ管理テーブル２１０に登録されたユーザ及び／又はその通信装置を識別する識別子を表している。ログイン用識別子は、ユーザが確認できるように、又は、好ましくは、ログイン画面２２１ａを受け取ったユーザ１０から隠された不可視の状態で、登録用画面２２１ａに埋め込まれている。ログイン用識別子２３２は登録用識別子２２２とは異なることが好ましい。なぜなら、本実施例では、上述したように、登録用識別子２２２はメーラー１６０によってユーザ１０に送られるものをそのまま使用しており、登録用識別子２２２は電子メールを介して暗号化されずにユーザ１０に送信されるため不正者によって読み盗られる可能性があるからである。ログイン用識別子２２３がログイン用画面２３１ａに既に埋め込まれているので、ユーザ１０はこれを入力及び管理する負担から開放される。フィールド２３３は、ユーザが予め任意に決定してユーザ管理テーブル２１０に登録した（例えば、８桁の）ログイン用パスワードを入力するフィールドである。ログイン用パスワードは登録用パスワードと同一であってもよいし、異なるパスワードであってもよい。フィールド２３４は、ユーザが登録用パスワードを入力し終わった後にこれを認証装置１００にウェブ通信により返信するためにクリックされるフィールドである。

【００４２】

図３（ｂ）を参照するに、ログイン画面２３１ｂは、メッセージ２３５と、「戻る」ボタン２３６のフィールドを有する。メッセージ２３５は、入力されたログイン用パスワードが間違っている旨及び再試行を促す旨をユーザ１０に表示する。「戻る」ボタン２３６は、ログイン画面２３１ｂを２３１ａに切り替えてユーザ１０にパスワードの再入力を可能にするボタンである。

【００４３】

以下、図４を参照して、認証システム１を利用してユーザ１０が認証装置１００によって認証を受ける場合の動作について説明する。ここで、図４は、認証システム１を利用してユーザ１０が認証装置１００によって認証を受ける場合の動作を説明するためのフローチャートである。ここでは、図１に示す携帯電話１０Ａを正規のユーザの携帯電話を表すものとし、携帯電話１０Ｂを不正者の携帯電話を表すものとする。

【００４４】

まず、ユーザ１０Ａは、認証装置１００の管理者にユーザ登録を当該携帯電話、ＦＡＸ及び郵送などを利用したオフラインで依頼する（ステップ１００２）。もっとも、ユーザ１０Ａが携帯電話とは別にデスクトップＰＣなどを有していればキーボード及びマウス等を利用した入力は容易であるから認証装置１００に直接オンラインでユーザ登録をすることができる。但し、この場合は携帯電話の方を登録する。

【００４５】

依頼を受けた認証装置１００又はその管理者は、ユーザ１０Ａから申し受けたユーザ情報（即ち、ユーザ１０Ａの氏名、住所、性別、年齢、誕生日、電話番号、電子メールアドレス、携帯電話の機種、（登録用及びログイン用）パスワードの検証用情報（パスワード自体であってもよいが、これを検証するのに必要なすべての情報を含む）、加入しているサービスの種類、必要な課金情報（銀行口座番号、クレジットカード番号など）、暗号用の鍵その他のＩＤ情報）の入力して記憶部２００のユーザ管理テーブル２１０に登録する（ステップ１００４）。登録の際、ＣＰＵ１１０は、ユーザ情報を暗号／復号化部１４０を介して暗号化し、又は、暗号化せずに、記憶部２００のユーザ管理テーブル２１０に格納する。

【００４６】

認証装置１００又はその管理者によるユーザ情報登録が完了すると、ＣＰＵ１１０は、登録用画面２２１のＵＲＬをメーラー１６０及び通信ポート１２０を介して携帯電話１０Ａの電子メールアドレスに送信すると共に対応する登録用画面２２１ａに登録用識別子２２２及び有効期限２２５を書き込む（ステップ１００６）。ＣＰＵ１１０は、登録用画面２２１のＵＲＬを送信する前に、予め記憶部

２００のユーザ管理テーブル２１０を参照し、携帯電話１０Ａの機種に閲覧可能な登録用画面２２１ａのＵＲＬを取得し、乱数発生部１３０を利用して当該携帯電話１０Ａを識別する登録用識別子をランダムに生成してこれを登録用画面２２１ａに含めておく。ＣＰＵ１１０が電子メールを提供するタイミングは認証装置１００へのユーザ情報登録完了時でもよいし、ユーザ１０からの要求時でもよい。

【００４７】

ユーザ１０Ａは、登録用画面２２１ａのＵＲＬを含む電子メールを受信すると（ステップ１００８）、登録用画面２２１ａを呼び出す（ステップ１０１０）。このとき、電子メールの中にＵＲＬが含まれているので、ユーザ１０Ａは携帯電話のキーパッドを使って、ＵＲＬを煩雑にも入力する必要がない。代わりに、ユーザ１０Ａは、電子メールのＵＲＬを反転させて携帯電話１０Ａに通常装備されている「決定キー」を押したり、ＵＲＬをクリック、ダブルクリック等したりすることによって登録用画面２２１ａＵＲＬを呼び出す。

【００４８】

これに応答して、ＣＰＵ１１０は対応する登録用画面２２１ａを表示する（ステップ１０１２）。ＣＰＵ１１０は、ＵＲＬの呼び出しがどの携帯電話機器の機種からのものであるか、ＵＲＬに含まれている機種特有の数値から判断する。登録用画面２２１ａには携帯電話１０Ａに固有の登録用識別子２２２が変更可能に書き込まれている。ＣＰＵ１１０は、登録用画面２２１ａを介してユーザ１０に登録用パスワードの入力を促す。通常、ＰＣのブラウザはウェブ通信及び電子メール通信の両方に暗号を使用することができるが、携帯電話では、ウェブ通信は暗号化が可能だが、電子メール通信の暗号化は行えない。このため、本実施例では、携帯電話の機種に特有の数値を含むＵＲＬを電子メールで提供する際に、盗聴され、ＵＲＬが漏洩する危険性があるため、パスワードを確認して、要求が正当なユーザ１０Ａからのものである確認をする。

【００４９】

その後、ユーザ１０Ａは登録用画面２２１ａの登録用パスワードをフィールド２２３に入力して認証装置１００に返信する（ステップ１０１４）。このときの

通信は、電子メール通信からウェブ通信に変わっており、登録用パスワードは暗号化されて送信され、盗聴されてパスワードが漏洩する危険性はない。

【００５０】

誤った登録用パスワードが入力されると登録用画面２２１ｂがユーザ１０Ａに送信され、登録用パスワードの再入力を促す。このとき、携帯電話１０Ａの置き忘れ、盗難等により、不正ユーザ１０Ｂの利用も考え、登録用パスワードを設定した回数連続して間違えると、当該登録用画面２２１ａが有効期間であっても使用できなくすることも可能である。フィールド２２５で規定された有効期限が過ぎていれば、登録用画面２２１ｃがユーザ１０Ａに送信され、その旨が通知される。この場合、ユーザ１０Ａは改めて認証装置１００又はその管理者にオンライン又はオフラインで連絡して新しい登録用画面２２１ａのＵＲＬを送信するように要求する。不正者１０ＢがＵＲＬと登録用パスワードを入手して登録用画面２２１ａのフィールド２２３に登録用パスワードを入力した場合、不正者の携帯電話１０Ｂが装置識別子を自動的に送信するものであれば登録用画面２２１ｄがユーザ１０Ｂに送信され、使用機種が違う旨を警告する。

【００５１】

ユーザ１０Ａが正しい登録用パスワードを有効期限内に認証装置１００に暗号化して送信すると、ＣＰＵ１１０は受け取った登録用パスワードを、暗号／復号化部１４０を介して復号化し、記憶部２００のユーザ管理テーブル２１０に格納されている登録用パスワードの検証用情報を参照してこれを検証する。検証が成功して、ＣＰＵ１１０がユーザ１０Ａを認証すると、ＣＰＵ１１０による登録制御は終了する（ステップ１０１６）。

【００５２】

次に、登録制御が終了して正規のユーザ１０Ａを認証すると、ＣＰＵ１１０はログイン画面２３１ａにログイン用識別子２３２を書き込んでユーザ１０Ａに送信する（ステップ１０１８）。上述したように、携帯電話の機種によっては装置識別子を自動的に送信するものがあるのでＣＰＵ１１０は、これをログイン用識別子２３２に設定することができるが、利用しなくても何ら問題なく、識別子を携帯電話機器自身で発行できるか否かで本発明が制限されるものではない。本実

施例では、ＣＰＵ１１０はログイン用識別子をユーザ１０Ａから隠れた状態でログイン画面２３１ａに埋め込み、ログイン画面２３１ａを暗号／復号化部１４０で暗号化してユーザ１０Ａに送信する。ログイン画面２３１ａは暗号化されて送信されるため、ログイン画面２３１ａに隠れた状態で埋め込まれているログイン用識別子２３２を盗聴され、それらが漏洩する危険性はない。

【００５３】

次いで、ユーザ１０Ａは、ログイン画面２３１ａを携帯電話１０Ａの画面メモ機能を利用して保存する（ステップ１０２０）。かかる処理は、ＰＣでは画面の保存に相当する。なお、ＣＰＵ１１０は、ユーザ１０Ａがステップ１０２０を行えることをユーザ管理テーブル２１０を参照して予め理解してステップ１０１８を行っている。

【００５４】

ユーザ１０Ａはアクセスをしたいときに、携帯電話機器上に保存されているログイン画面を呼び出し（ステップ１０２２）、ログイン用パスワード２３３を入力して認証装置１００に送信する。ユーザ１０の識別子が予めログイン画面に埋め込まれているので、ユーザ１０はログイン画面２３１ａで新たに識別情報を入力する必要はなく、キー操作が容易である。上述したように、ログイン用パスワード２３３は登録用パスワードと同一でも相違してもよい。ユーザ１０から認証装置１００へのログイン画面の送信もウェブ上で行っているため、ログイン画面２３１ａの内容は暗号化されており、ユーザ１０の識別情報及びログイン用パスワードが盗聴されて漏洩する危険性はない。

【００５５】

誤ったログイン用パスワード２３３が入力されるとログイン画面２３１ｂがユーザ１０Ａに送信され、ログイン用パスワード２３３の再入力を促す。

【００５６】

ユーザ１０Ａが正しいログイン用パスワード２３３を認証装置１００に暗号化して送信すると、ＣＰＵ１１０は受け取ったログイン用パスワード２３３を、暗号／復号化部１４０を介して復号化し、記憶部２００のユーザ管理テーブル２１０に格納されているログイン用パスワードの検証用情報を参照してこれを検証す

る。検証が成功して、ＣＰＵ１１０がユーザ１０Ａを認証すると、ＣＰＵ１１０によるログイン制御は終了する（ステップ１０２６）。その後、ＣＰＵ１１０は、ユーザ１０Ａを情報提供装置２０にアクセスすることを可能にする。この結果、ユーザ１０Ａは、容易なキー操作によって情報提供装置２０の情報にアクセスすることができる。

【００５７】

図５に、図４の変形例を示す。図５においては、ＣＰＵ１１０は、ユーザ１０Ａがステップ１０２０を行えず、ログイン画面のＵＲＬのブックマークのみを行えることをユーザ管理テーブル２１０を参照して予め認識している。このため、ステップ１０１８の代わりに、ログイン用識別子２３２を含んだログイン画面２３１ａのＵＲＬを送信する（ステップ１０２８）。これに応答して、ユーザ１０Ａは、かかるＵＲＬをブックマークする（ステップ１０３０）。ユーザ１０Ａはアクセスをしたいときに、携帯電話にそのＵＲＬがブックマークされているログイン画面２３１ａを呼び出し（ステップ１０３２）、認証装置１１０にログイン画面２３１ａを表示させ（ステップ１０３４）、ステップ１０２４に至る。

【００５８】

以上、本発明の好ましい実施例を説明したが、本発明はその要旨の範囲内で様々な変形や変更が可能である。

【００５９】

【発明の効果】

本発明の認証方法及び装置は、ユーザ、特に、キー入力が煩雑な通信装置を使用するユーザに対して、容易、安価、且つ、セキュリティに優れた確実な本人認証動作を提供する。

【図面の簡単な説明】

【図１】　本発明の認証システムのシステム構成図である。

【図２】　図１に示す認証システムの認証装置が使用する登録用画面の概略図である。

【図３】　図１に示す認証システムの認証装置が使用するログイン用画面の概略図である。

【図４】　図１に示す認証システムの動作を説明するためのフローチャートである。

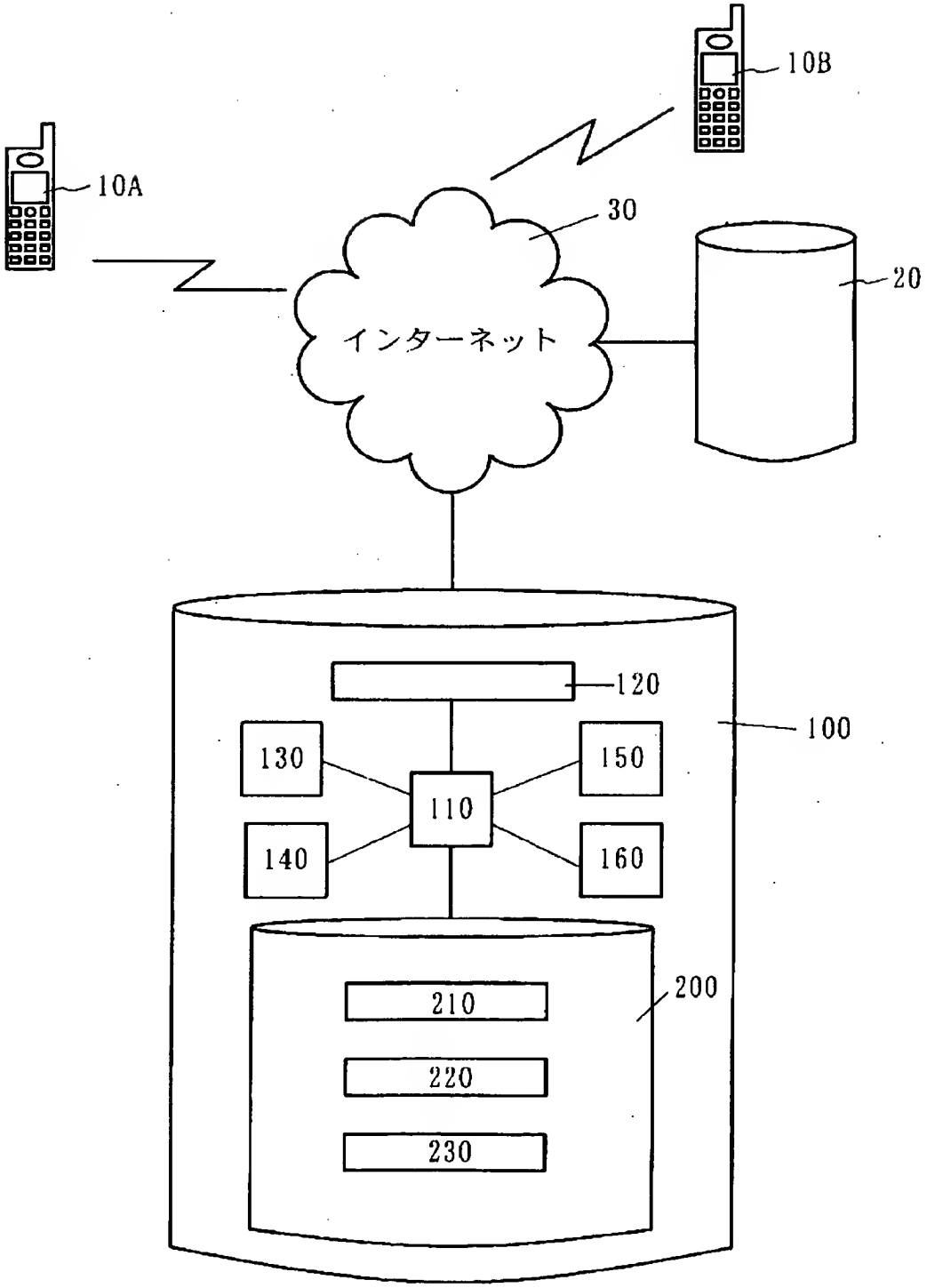
【図５】　図４に示すフローチャートの変形例である。

【符号の説明】

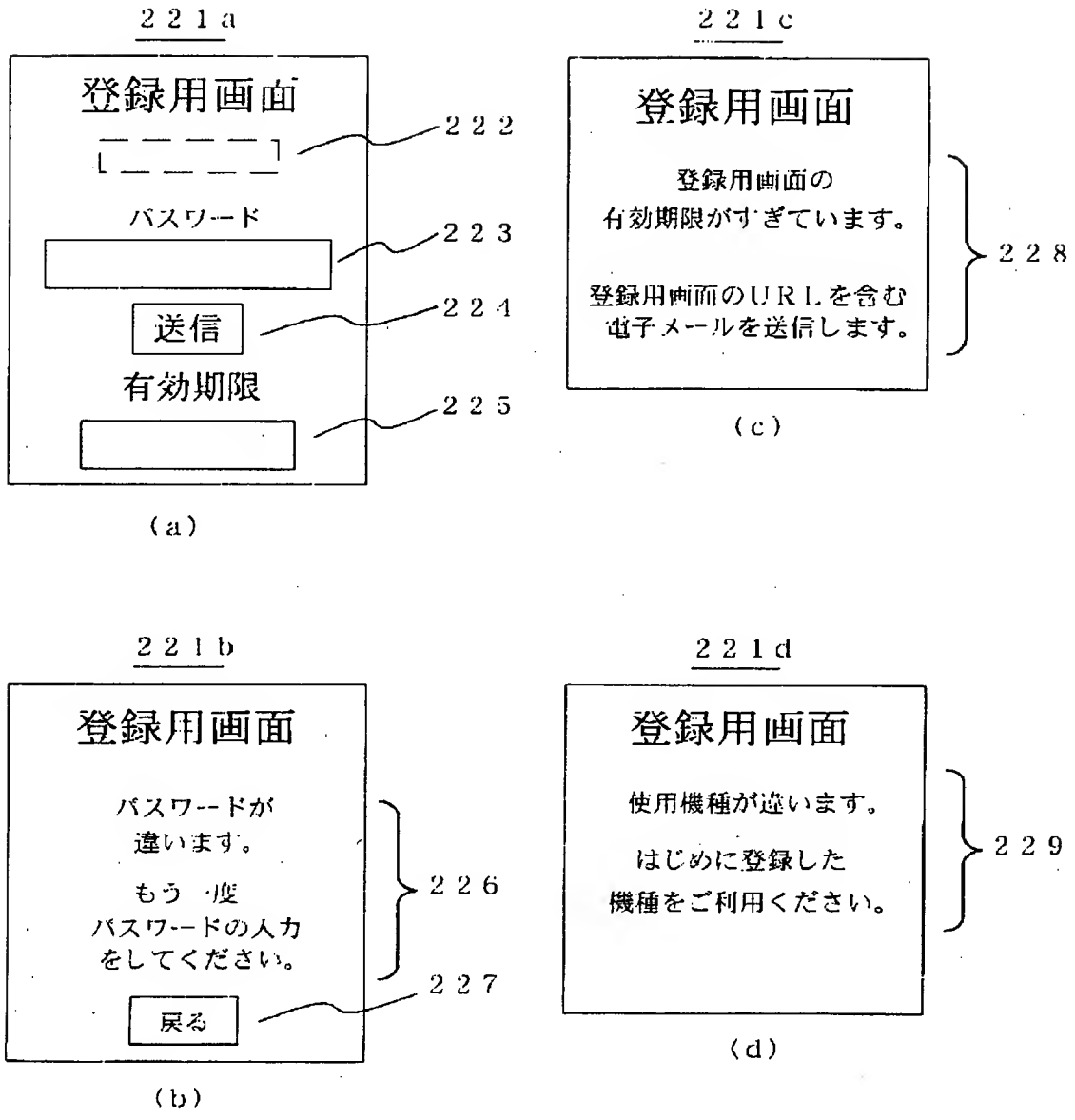
１	認証システム
１０Ａ	ユーザ（及び／又はその携帯電話）
１０Ｂ	不正ユーザ（及び／又はその携帯電話）
２０	情報提供装置
３０	インターネット
１００	認証装置
１１０	制御部
１２０	通信ポート
１３０	乱数発生部
１４０	暗号／復号化部
１５０	メモリ
２００	記憶装置
２１０	ユーザ管理テーブル
２２０	登録用画面保管テーブル
２３０	ログイン画面管理テーブル

【書類名】　　図面

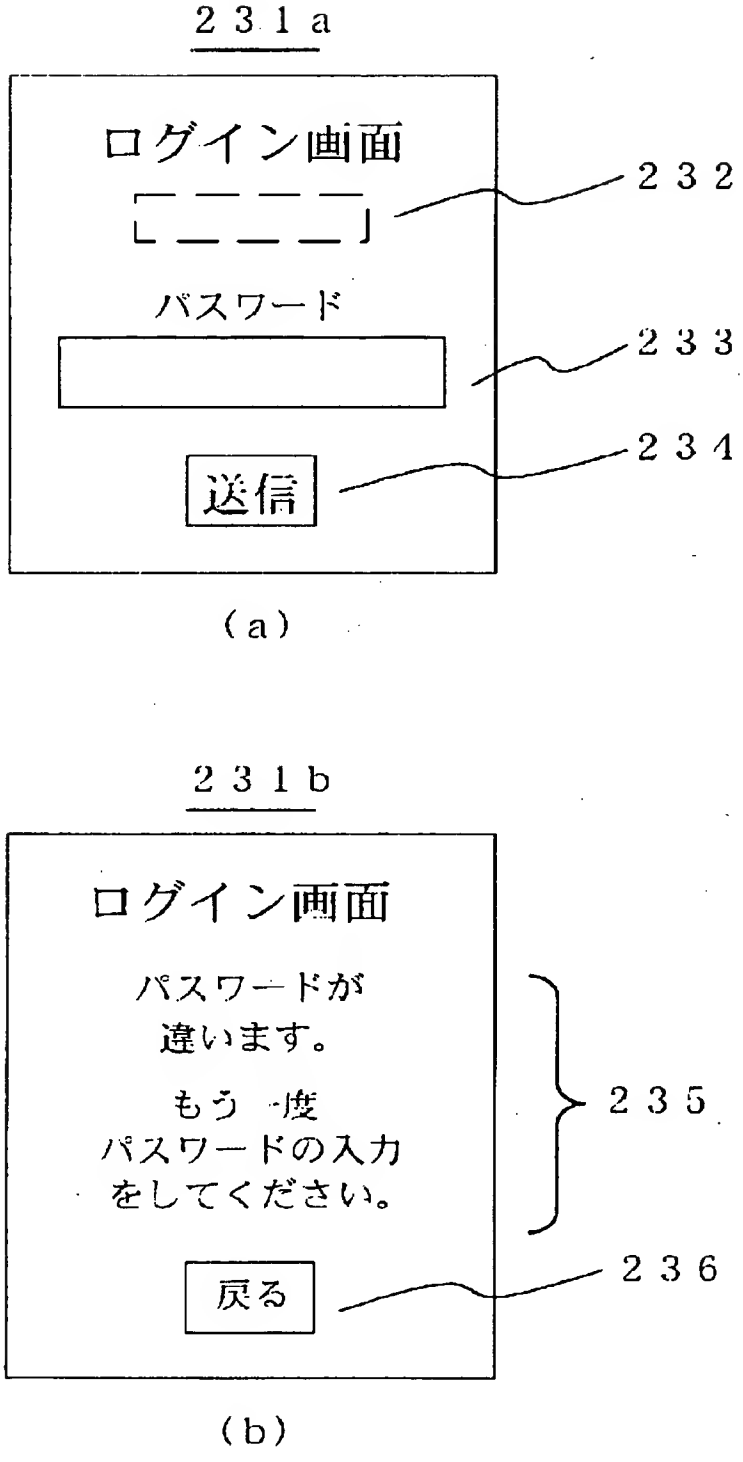
【図１】


10B
10A
30
20
インターネット
120
100
130
150
110
140
160
200
210
220
230

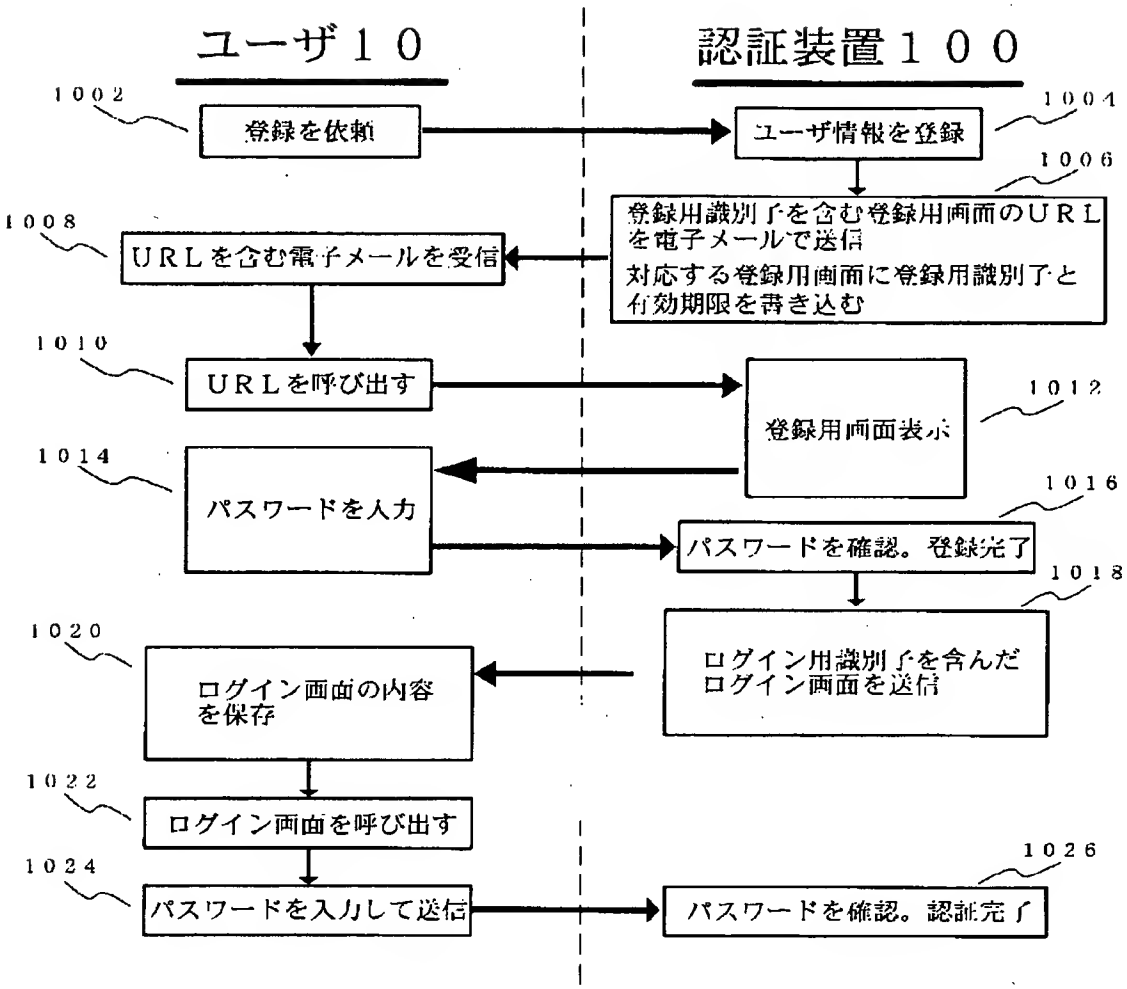
【図２】


２２１ａ
登録用画面
２２２
パスワード
２２３
送信
２２４
有効期限
２２５
（ａ）
２２１ｃ
登録用画面
登録用画面の
有効期限がすぎています。
登録用画面のＵＲＬを含む
電子メールを送信します。
２２８
（ｃ）
２２１ｂ
登録用画面
パスワードが
違います。
もう一度
パスワードの入力
をしてください。
２２６
２２７
戻る
（ｂ）
２２１ｄ
登録用画面
使用機種が違います。
はじめに登録した
機種をご利用ください。
２２９
（ｄ）

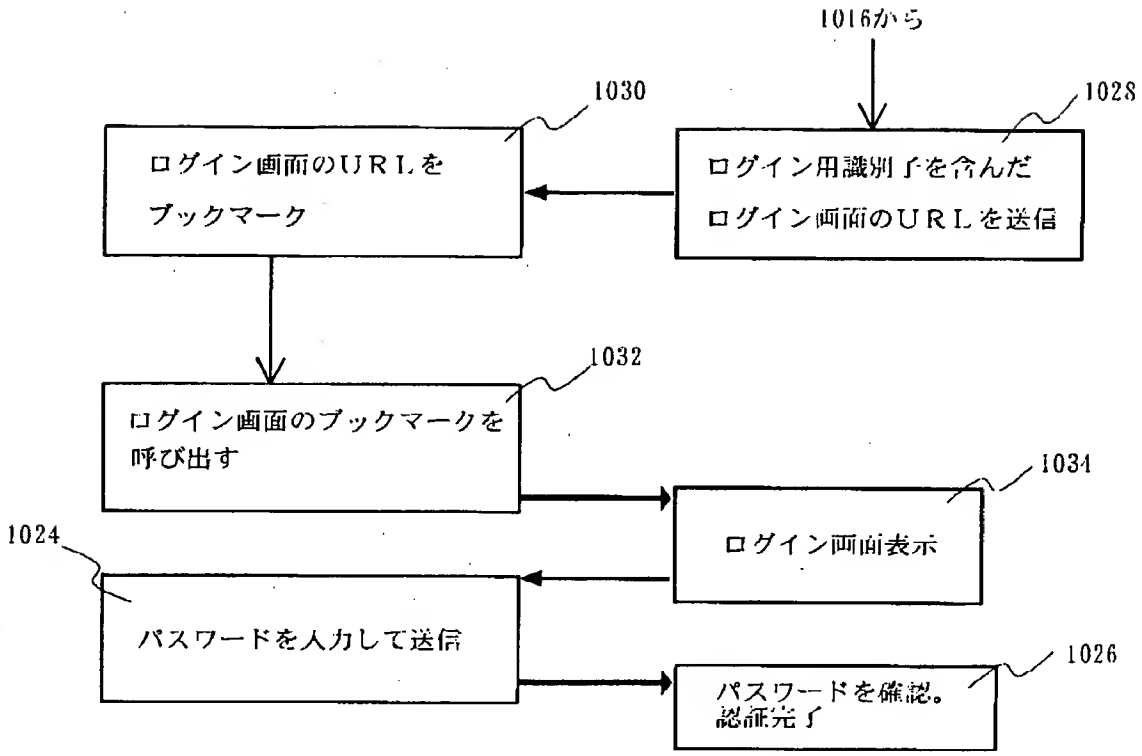
【図３】


２３１ａ
ログイン画面
２３２
パスワード
２３３
送信
２３４
（ａ）
２３１ｂ
ログイン画面
パスワードが
違います。
もう一度
パスワードの入力
をしてください。
２３５
戻る
２３６
（ｂ）

【図４】


ユーザ１０
認証装置１００
1002
登録を依頼
1004
ユーザ情報を登録
1006
登録用識別子を含む登録用画面のＵＲＬを電子メールで送信
対応する登録用画面に登録用識別子と有効期限を書き込む
1008
ＵＲＬを含む電子メールを受信
1010
ＵＲＬを呼び出す
1012
登録用画面表示
1014
パスワードを入力
1016
パスワードを確認。登録完了
1018
ログイン用識別子を含んだログイン画面を送信
1020
ログイン画面の内容を保存
1022
ログイン画面を呼び出す
1024
パスワードを入力して送信
1026
パスワードを確認。認証完了

【図５】


1016から
1030
1028
ログイン画面のＵＲＬを
ブックマーク
ログイン用識別子を含んだ
ログイン画面のＵＲＬを送信
1032
ログイン画面のブックマークを
呼び出す
1034
ログイン画面表示
1024
パスワードを入力して送信
1026
パスワードを確認。
認証完了

【書類名】　　要約書

【要約】

【課題】　本発明の本人認証及び認証装置は、ユーザが容易、安価、且つ、セキュリティに優れた確実な本人認証が行えるサービスを提供することを目的とする。

【解決手段】　本発明の認証方法は、ユーザの通信装置に前記ユーザ及び／又は前記通信装置固有の登録用画面のアドレスに前記ユーザ及び／又は前記通信装置を識別する登録用識別子を含めて送信するステップと、前記アドレスがアクセスされて前記登録用画面に第１のパスワードが入力されて返信された場合に前記登録用識別子と前記第１のパスワードに基づいて前記ユーザを認証するステップと、前記認証ステップが成功した場合に、ログイン画面を前記ユーザに送信するステップであって、前記ログイン画面は、第２のパスワードが入力されるフィールドと、前記ユーザ及び／又は前記通信装置を識別するログイン用識別子とを有するステップと、前記ユーザにより返信された前記ログイン画面に含まれる前記ログイン用識別子と前記第２のパスワードに基づいて前記ユーザを認証するステップとを有する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－４０２１５２
受付番号	５００００１７０５１９８
書類名	特許願
担当官	佐藤　一博　　１９０９
作成日	平成１３年　１月１０日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	501005807
【住所又は居所】	東京都渋谷区恵比寿４－２０－３ＹＧＰタワー
【氏名又は名称】	モルガン・スタンレー・ディーン・ウィッター・ジャパン・リミテッド

【代理人】　申請人

【識別番号】	100110412
【住所又は居所】	東京都中央区八丁堀四丁目９番４号　東京ＳＴビル９階佐藤・藤元特許事務所
【氏名又は名称】	藤元　亮輔

次頁無

認定・付加情報

特許出願の番号	特願２０００－４０２１５２
受付番号	５００００１７０５１９８
書類名	特許願
担当官	佐藤　一博　　１９０９
作成日	平成１３年　３月２７日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	501005807
【住所又は居所】	東京都渋谷区恵比寿４－２０－３ＹＧＰタワー
【氏名又は名称】	モルガン・スタンレー・ディーン・ウィッター・ジャパン・リミテッド

【代理人】

【識別番号】	100110412
【住所又は居所】	東京都中央区八丁堀四丁目９番４号　東京ＳＴビル９階佐藤・藤元特許事務所
【氏名又は名称】	藤元　亮輔

次頁無

【書類名】　手続補正書
【あて先】　特許庁長官殿
【事件の表示】
　【出願番号】　特願2000-402152
【補正をする者】
　【識別番号】　501005807
　【氏名又は名称】　モルガン・スタンレー・ディーン・ウィッター・ジャパン・リミテッド
　【代表者】　可児　武夫
【代理人】
　【識別番号】　100110412
　【弁理士】
　【氏名又は名称】　藤元　亮輔
【発送番号】　018695
【手続補正　1】
　【補正対象書類名】　特許願
　【補正対象項目名】　特許出願人
　【補正方法】　変更
　【補正の内容】
　　【特許出願人】
　　【識別番号】　501005807
　　【住所又は居所】　ケイマン諸島、グランドケイマン、ジョージダウン、サウスチャーチ・ストリート、ユグランドハウス、私書箱３０９号
　　【氏名又は名称】　モルガン・スタンレー・ディーン・ウィッター・ジャパン・リミテッド
　　【営業所】　東京都渋谷区恵比寿四丁目２０番３号恵比寿ガーデンプレイスタワー
　　【代表者】　可児　武夫

【プルーフの要否】　要

認定・付加情報

特許出願の番号	特願２０００－４０２１５２
受付番号	５０１００３７０１３８
書類名	手続補正書
担当官	佐藤　一博　　１９０９
作成日	平成１３年　３月２７日

＜認定情報・付加情報＞

【提出日】	平成13年 3月15日
【補正をする者】	
【識別番号】	501005807
【住所又は居所】	東京都渋谷区恵比寿４－２０－３ＹＧＰタワー
【氏名又は名称】	モルガン・スタンレー・ディーン・ウィッター・ジャパン・リミテッド
【代理人】	申請人
【識別番号】	100110412
【住所又は居所】	東京都中央区八丁堀四丁目９番４号　東京ＳＴビル９階佐藤・藤元特許事務所
【氏名又は名称】	藤元　亮輔

次頁無

出　願　人　履　歴　情　報

識別番号　　〔５０１００５８０７〕

１．変更年月日　　２０００年１２月２８日
［変更理由］　新規登録
住　所　東京都渋谷区恵比寿４－２０－３ＹＧＰタワー
氏　名　モルガン・スタンレー・ディーン・ウィッター・ジャパン・リミテッド

２．変更年月日　　２００１年　５月１８日
［変更理由］　住所変更
住　所　ケイマン諸島、グランドケイマン、ジョージダウン、サウスチャーチ・ストリート、ユグランドハウス、私書箱３０９号
氏　名　モルガン・スタンレー・ディーン・ウィッター・ジャパン・リミテッド